THE REMAINING 40% OF RAMANUJAN'S LOST NOTEBOOK (Number Theory and its Applications)

AUTHOR(S):

Berndt, Bruce C.

数理解析研究所講究録
1060巻 1998年 111-118

THE REMAINING 40% OF RAMANUJAN'S LOST NOTEBOOK

BRUCE C. BERNDT

To provide the setting for the material discussed in the sequel, we briefly describe the history of Ramanujan's lost notebook. It will be convenient to begin in the year 1976 and then proceed backward.

In the spring of 1976, George Andrews visited Trinity College, Cambridge, to examine the papers left by G. N. Watson. Among Watson's papers, he found a manuscript containing 138 pages in the handwriting of Ramanujan. In view of the fame of Ramanujan's notebooks, published in a photocopy edition by the Tata Institute of Fundamental Research in Bombay in 1957 [14], it was natural to call this newly found manuscript "Ramanujan's lost notebook." How did this manuscript reach Trinity College?

Watson died in 1965 at the age of 79. Shortly thereafter, on separate occasions, J. M. Whittaker and R. A. Rankin visited Mrs. Watson. The late J. M. Whittaker was a physicist and son of E. T. Whittaker, who coauthored with Watson probably the most popular and frequently used text on analysis in the 20th century [25]. Rankin, who has been at the University of Glasgow for many years, had succeeded Watson as Professor of Mathematics at the University of Birmingham, where Watson served for most of his career. Both Whittaker and Rankin went to Watson's attic office to examine the papers left by him, and both found the aforementioned manuscript by Ramanujan. Rankin suggested to Mrs. Watson that her late husband's papers be sorted and sent to Trinity College Library, Cambridge, for preservation. During the next three years, Rankin sent Watson's papers, including the Ramanujan manuscript, sent on 26 December 1968, in batches to Trinity's library. Rankin had not realized the importance of Ramanujan's manuscript and so did not mention it to anyone. In particular, he did not reveal the manuscript's existence in his obituary [17] of Watson written for the *London Mathematical Society*. Thus, the next question is: How did Watson come into possession of this sheaf of 138 pages of Ramanujan's work?

After Ramanujan died in 1920, G. H. Hardy strongly urged that Ramanujan's published papers, notebooks, and other unpublished work be collected together for publication. A handwritten copy of Ramanujan's notebooks [14] was shipped from the University of Madras to Hardy in 1923, and at the same time other manuscripts and papers of Ramanujan were also sent. There apparently is no record of precisely what was included in this shipment. Thus, most likely, the lost notebook was sent to Hardy in 1923.

In the 1920s and 1930s, Watson wrote almost 40 papers on the work of Ramanujan, most of them arising from either Ramanujan's letters to Hardy or from

Ramanujan's notebooks. In particular, he wrote on Ramanujan's mock theta functions, which Ramanujan discovered in the last year of his life and described in a letter to Hardy only about three months before he died [7, pp. 220–223]. Watson had made some conjectures on the existence of certain mock theta functions. If he had had in his possession the lost notebook, he would have seen that his conjectures were correct. Thus, probably sometime after Watson's interest in Ramanujan's work waned in the late 1930s, but before his death in 1947, Hardy passed Ramanujan's manuscript to Watson. Since many identities involving mock theta functions appear in the lost notebook, it is certain that the lost notebook arises from the last year of Ramanujan's life.

Finally, in early 1988, just after the centenary of Ramanujan's birth, Narosa Publishing House in New Delhi published a photocopy edition of the lost notebook [16]. Included in the edition are a few other unpublished manuscripts by Ramanujan as well as letters between Ramanujan and Hardy. Shortly thereafter, Rankin wrote a very interesting paper on the origin and content of the lost notebook, as well as other manuscripts left by Ramanujan [18].

About 60% of the approximately 650 claims made by Ramanujan in his lost notebook pertain to mock theta functions and other q–series. Most of these results have now been proved by Andrews. We cite just one of his papers [1], which provides some of the lost notebook's history that we have related above. The remaining 40% is devoted mostly to topics examined by Ramanujan in the ordinary notebooks. For example, theta function identities, modular equations, Eisenstein series, integrals of theta functions, incomplete elliptic integrals of the first kind, the Rogers–Ramanujan continued fraction, and other continued fractions are some of the topics found in the lost notebook. This 40% (as well as the other 60%) is of great interest to the present author. In the remainder of this paper, we briefly describe some of these results. Much of the research on these entries is being conducted with the author's recent and current graduate students, in particular, Heng Huat Chan, Sen–Shan Huang, Soon–Yi Kang, Wen–Chin Liaw, Jaebum Sohn, Seung Hwan Son, and Liang–Cheng Zhang.

Definitions

As customary, set

$$(a;q)_\infty := \prod_{n=0}^{\infty}(1-aq^n), \qquad |q|<1.$$

Ramanujan's general theta function $f(a,b)$, which has the same generality as the general classical theta function, as found in [25, Chap. 21], for example, is defined by

$$f(a,b) := \sum_{n=-\infty}^{\infty} a^{n(n+1)/2}b^{n(n-1)/2}, \qquad |ab|<1. \tag{1}$$

In Ramanujan's notation, the three most important special cases of (1) are

$$\varphi(q) := f(q,q) = \sum_{n=-\infty}^{\infty} q^{n^2},$$

$$\psi(q) := \frac{1}{2} f(q,1) = \sum_{n=0}^{\infty} q^{n(n+1)/2},$$

and

$$(2) \qquad f(-q) := f(-q,-q^2) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(3n-1)/2} = (q;q)_\infty =: q^{-1/24}\eta(\tau),$$

where $q = \exp(2\pi i\tau)$, $\operatorname{Im}\tau > 0$, and η denotes the Dedekind eta-function. The penultimate equality in (2) is Euler's pentagonal number theorem.

If $q = \exp(-\pi\sqrt{n})$, for some positive rational number n, The Ramanujan–Weber class invariant G_n is defined by

$$(3) \qquad G_n := 2^{-1/4} q^{-1/24} (-q;q^2)_\infty.$$

The Rogers–Ramanujan continued fraction $R(q)$ is defined by

$$(4) \qquad R(q) := \frac{q^{\frac{1}{5}}}{1} \; \frac{q}{1} + \frac{q^2}{1} + \frac{q^3}{1} + \cdots, \qquad |q| < 1.$$

Theta Function Identities

In his lost notebook, Ramanujan refined or factored some of the theta function identities recorded by him in his notebooks. For example, in his notebooks [2, p. 262, Entry 10], Ramanujan recorded the identity

$$\varphi^2(q) - 5\varphi^2(q^5) = -4f^2(-q^2)\frac{(-q^5;q^{10})_\infty}{(-q;q^2)_\infty}.$$

On page 56 in his lost notebook, he factored this identity into the following identities: If $\alpha = \frac{1-\sqrt{5}}{2}$ and $\beta = \frac{1+\sqrt{5}}{2}$, then

$$\varphi(q) + \sqrt{5}\varphi(q^5) = \frac{(1+\sqrt{5})f(-q^2)}{\prod_{n\,\text{odd}} (1+\alpha q^n + q^{2n}) \prod_{n\,\text{even}} (1-\beta q^n + q^{2n})},$$

$$\varphi(q) - \sqrt{5}\varphi(q^5) = \frac{(1-\sqrt{5})f(-q^2)}{\prod_{n\,\text{even}} (1-\alpha q^n + q^{2n}) \prod_{n\,\text{odd}} (1+\beta q^n + q^{2n})}.$$

In his notebooks [3, pp. 12, 13, Entry 1], Ramanujan introduced the parameter

$$k := R(q)R^2(q^2),$$

and stated two elegant modular equations,

$$R^5(q) = k\left(\frac{1-k}{1+k}\right)^2 \qquad \text{and} \qquad R^5(q^2) = k^2\left(\frac{1+k}{1-k}\right).$$

In his lost notebook, Ramanujan gives several other beautiful identities involving the parameter k, for example,

$$\frac{k}{1-k^2}\left(\frac{1+k-k^2}{1-4k-k^2}\right)^5 = q(-q;q)_\infty^{24}.$$

Thus, Ramanujan has given a beautiful paramtrization for the discrimiant function, $\Delta(\tau) := q(q:q)_\infty^{24}$, where $q = \exp(2\pi i\tau)$.

Proofs of the results cited above have been given by Kang [11].

On page 206 in his lost notebook, Ramanujan gave a very strange sequence of septic identities, which we now quote. Let

$$\frac{\varphi(q^{1/7})}{\varphi(q^7)} = 1 + u + v + w.$$

Then

$$p = uvw = \frac{8q^2(-q;q^2)_\infty}{(-q^7;q^{14})_\infty^7} \tag{5}$$

and

$$\frac{\varphi^8(q)}{\varphi^8(q^7)} - (2+5p)\frac{\varphi^4(q)}{\varphi^4(q^7)} + (1-p)^3 = 0.$$

Furthermore,

$$u = \left(\frac{\alpha^2 p}{\beta}\right)^{1/7}, \quad v = \left(\frac{\beta^2 p}{\gamma}\right)^{1/7}, \quad w = \left(\frac{\gamma^2 p}{\alpha}\right)^{1/7},$$

where α, β, and γ are roots of the equation

$$x^3 + 2x^2\left(1 + 3p - \frac{\varphi^4(q)}{\varphi^4(q^7)}\right) + xp^2(p+4) - p^4 = 0.$$

For example,

$$\varphi(e^{-7\pi\sqrt{7}}) = 7^{3/4}\varphi(e^{-\pi\sqrt{7}})\left\{1 + (-)^{2/7} + (-)^{2/7} + (-)^{2/7}\right\}. \tag{6}$$

Although u, v, and w are not given by Ramanujan, they are given in Entry 17(iii) in Chapter 19 of Ramanujan's second notebook [2, p. 303]. Explicitly,

$$u = 2q^{1/7}\frac{f(q^5,q^9)}{\varphi(q^7)}, \qquad v = 2q^{4/7}\frac{f(q^3,q^{11})}{\varphi(q^7)}, \qquad \text{and} \qquad w = 2q^{9/7}\frac{f(q,q^{13})}{\varphi(q^7)}.$$

Equality (5) is easy to prove, but the proofs of the remaining identities are very difficult. Except for (6), Son [22] has found proofs of the remaining claims. Did Ramanujan have explicit identifications for the three missing expressions in (6), or did he merely conjecture that there exists a representation for $\varphi(e^{-7\pi\sqrt{7}})$ in the form (6)? It seems to us that if Ramanujan were able to complete this entry, he would have needed to know the value of the class invariant (see (3)) G_{343}, which apparently he did not know, and which we also do not know.

The papers by Kang [10], [11] and Son [20]–[23] contain proofs of several further theta function identities from the lost notebook.

Lambert Series

Pages 353–357 in the publication of the lost notebook [16] comprise a summary of some of Ramanujan's findings about Lambert series. The paper that we will write for the published proceedings of the *RIMS Symposium on Number Theory* will concentrate on this fragment. Here we cite only two examples.

Beginning with the work of Gauss, Legendre, and Jacobi, Lambert series have been useful in deriving formulas for the number of representations of a positive integer n by certain quadratic forms. For example, if $r_k(n)$ denotes the number of ways of representing the positive integer n as a sum of k squares, then the Lambert series identity

$$\varphi^8(q) = 1 + 16 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-(-q)^n},$$

due to Jacobi, yields the formula

$$r_8(n) = 16(-1)^n \sum_{d|n} (-1)^d d^3.$$

Similarly, let $t_k(n)$ denote the number of ways that the positive integer n can be represented as a sum of k triangular numbers. Then the Lambert series identity

$$q^{3/2}\psi^6(q^2) = \frac{1}{16} \sum_{n=0}^{\infty} \frac{(2n+1)^2 q^{(2n+1)/2}}{1+q^{2n+1}} - \frac{1}{16} \sum_{n=0}^{\infty} \frac{(-1)^n (2n+1)^2 q^{(2n+1)/2}}{1-q^{2n+1}}$$

gives the corollary

$$t_6(n) = \frac{1}{8} \sum_{\substack{d|(4n+3) \\ d \equiv 3 \pmod 4}} d^2 - \frac{1}{8} \sum_{\substack{d|(4n+3) \\ d \equiv 1 \pmod 4}} d^2.$$

We have been unable to find this formula in the classical literature. The first occurrences known to us are in recent papers by Kac and Wakimoto [9] and by Ono, Robins, and Wahl [12]. We have found a proof along the lines of Ramanujan's thinking.

Incomplete Elliptic Integrals of the First Kind

Some of the most amazing formulas in the lost notebook involve incomplete elliptic integrals. We cite just one of several examples. Recall that $f(-q)$ is defined by (2).

If

$$v := q \frac{f^3(-q) f^3(-q^{15})}{f^3(-q^3) f^3(-q^5)},$$

then

$$(7) \quad \int_0^q f(-t) f(-t^3) f(-t^5) f(-t^{15}) dt = \frac{1}{5} \int_{2\arctan\left(\frac{1}{\sqrt{5}} \sqrt{\frac{1-11v-v^2}{1+v-v^2}}\right)}^{2\arctan(1/\sqrt{5})} \frac{dt}{\sqrt{1-\frac{9}{25}\sin^2 t}}.$$

This and several other formulas in the lost notebook of the same sort were first proved by Raghavan and Rangachari [13]. However, their proofs partially depend upon ideas with which Ramanujan would not have been familiar. In particular, to prove (7), they used the remarkable differential equation

$$\frac{dv}{dq} = f(-q)f(-q^3)f(-q^5)f(-q^{15})\sqrt{1-10v-13v^2+10v^3+v^4}, \tag{8}$$

which they quote from the treatise of Fricke [8, p. 439]. The author, H. H. Chan, and S.-S. Huang in an unpublished manuscript have given more elementary proofs of (7) and (8).

The Rogers–Ramanujan Continued Fraction

Recall that the Rogers–Ramanujan continued fraction $R(q)$ is defined by (4). Using the Rogers–Ramanujan identities, we obtain the beautiful representation

$$q^{-1/5}R(q) = \frac{(q;q^5)_\infty (q^4;q^5)_\infty}{(q^2;q^5)_\infty (q^3;q^5)_\infty}. \tag{9}$$

But perhaps the most important and useful theorem about $R(q)$ is given by the formula

$$\frac{1}{R(q)} - 1 - R(q) = \frac{f(-q^{1/5})}{q^{1/5}f(-q^5)}, \tag{10}$$

where $f(-q)$ is defined by (2). The corollary,

$$\frac{1}{R^5(q)} - 11 - R^5(q) = \frac{f^6(-q)}{qf^6(-q^5)}, \tag{11}$$

is also very useful. These results are found in Ramanujan's second notebook [14, pp. 265–267] and were first proved by Watson [24] for the purpose of establishing some of Ramanujan's claims about $R(q)$ made in his first two letters to Hardy [15, pp. xxvii, xxviii]. They were also crucially used by the author, Chan, and Zhang [5] in deriving general formulas for the explicit evaluation of $R(q)$. As we shall see in the next paragraphs, Ramanujan recorded two-variable generalizations of (10) and (11) in his lost notebook.

On page 207 in his lost notebook, Ramanujan listed three identities,

$$P - Q = 1 + \frac{f(-q^{1/5}, -\lambda q^{2/5})}{q^{1/5}f(-\lambda^{10}q^5, -\lambda^{15}q^{10})}, \tag{12}$$

$$PQ = 1 - \frac{f(-\lambda, -\lambda^4 q^3)f(-\lambda^2 q, -\lambda^3 q^2)}{f^2(-\lambda^{10}q^5, -\lambda^{15}q^{10})}, \tag{13}$$

$$P^5 - Q^5 = 1 + 5PQ + 5P^2Q^2 + \frac{f(-q, -\lambda^5 q^2)f^5(-\lambda^2 q, -\lambda^3 q^2)}{q\, f^6(-\lambda^{10}q^5, -\lambda^{15}q^{10})}, \tag{14}$$

without specifying the functions P and Q. Son [19] has been able to discern the identities of P, Q, and R, and so prove the following theorem. If

$$P = \frac{f(-\lambda^{10}q^7, -\lambda^{15}q^8) + \lambda q f(-\lambda^5 q^2, -\lambda^{20}q^{13})}{q^{1/5} f(-\lambda^{10}q^5, -\lambda^{15}q^{10})}, \tag{15}$$

$$Q = \frac{\lambda f(-\lambda^5 q^4, -\lambda^{20}q^{11}) - \lambda^3 q f(-q, -\lambda^{25}q^{14})}{q^{-1/5} f(-\lambda^{10}q^5, -\lambda^{15}q^{10})}, \tag{16}$$

then (12)–(14) hold.

By setting $\lambda = 1$, in (15) and (16), using the quintuple product identity

$$f(-\lambda^2 x^3, -\lambda x^6) + x f(-\lambda, -\lambda^2 x^9) = \frac{f(-x^2, -\lambda x) f(-\lambda x^3)}{f(-x, -\lambda x^2)},$$

with $(x, \lambda) = (q, q^2)$ and (q^2, q^{-1}), respectively, employing Jacobi's triple product identity, and utilizing (9), we see that

$$P = \frac{f(-q^7, -q^8) + q f(-q^2, -q^{13})}{q^{1/5} f(-q^5)} = \frac{f(-q^2, -q^3)}{q^{1/5} f(-q, -q^4)} = \frac{1}{R(q)}, \tag{17}$$

$$Q = \frac{f(-q^4, -q^{11}) - q f(-q, -q^{14})}{q^{-1/5} f(-q^5)} = \frac{q^{1/5} f(-q, -q^4)}{f(-q^2, -q^3)} = R(q). \tag{18}$$

Since $PQ = 1$, from (17), (18), and (2), we see that (12) and (14) reduce to the two main identities, (10) and (11), respectively.

We close with a beautiful transformation for a generalization of the Rogers–Ramanujan continued fraction found on page 46 of the lost notebook.

Let $k \geq 0, \alpha = (1 + \sqrt{1+4k})/2$, and $\beta = (-1 + \sqrt{1+4k})/2$. Then, for $|q| < 1$ and Re $q > 0$,

(17)

$$\frac{1}{1} + \frac{k+q}{1} + \frac{k+q^2}{1} + \frac{k+q^3}{1} + \cdots = \frac{1}{\alpha} + \frac{q}{\alpha+\beta q} + \frac{q^2}{\alpha+\beta q^2} + \frac{q^3}{\alpha+\beta q^3} + \cdots.$$

In particular, if $k = 2$, we obtain the following elegant corollary, also found on page 46, but with a slight misprint. For $|q| < 1$,

$$\frac{1}{1} + \frac{2+q}{1} + \frac{2+q^2}{1} + \frac{2+q^3}{1} + \cdots = \frac{1}{2} + \frac{q}{2+q} + \frac{q^2}{2+q^2} + \frac{q^3}{2+q^3} + \cdots.$$

For proofs of many results on the Rogers–Ramanujan continued fraction found in the lost notebook, see a paper by the author, Huang, Sohn, and Son [6], and for a survey on the Rogers–Ramanujan continued fraction, with emphasis on results in the lost notebook, see [4].

References

1. G. E. Andrews, *An introduction to Ramanujan's "lost" notebook*, Amer. Math. Monthly **86** (1979), 89–108.
2. B. C. Berndt, *Ramanujan's Notebooks, Part III*, Springer-Verlag, New York, 1991.

3. B. C. Berndt, *Ramanujan's Notebooks, Part V*, Springer–Verlag, New York, 1997.
4. B. C. Berndt, H. H. Chan, S.–S. Huang, S.–Y. Kang, J. Sohn, and S. H. Son, *The Rogers–Ramanujan continued fraction* (to appear).
5. B. C. Berndt, H. H. Chan, and L.–C. Zhang, *Explicit evaluations of the Rogers–Ramanujan continued fraction*, J. Reine Angew. Math. **480** (1996), 141–159.
6. B. C. Berndt, S.–S. Huang, J. Sohn, and S. H. Son, *Some theorems on the Rogers–Ramanujan continued fraction in Ramanujan's lost notebook* (to appear).
7. B. C. Berndt and R. A. Rankin, *Ramanujan: Letters and Commentary*, Amer. Math. Soc., Providence, 1995; London Math. Soc., London, 1995.
8. R. Fricke, *Die Elliptische Funktionen und ihre Anwendungen, Bd. II*, Teubner, Leipzig, 1922.
9. V. G. Kac and M. Wakimoto, *Integrable highest weight modules over affine superalgebras and number theory*, Lie Theory and Geometry (J.–L. Brylinski, R. Brylinski, V. Guillemin, and V. Kac, eds.), Birkhäuser, Boston, 1994.
10. S.–Y. Kang, *Some theorems on the Rogers–Ramanujan continued fraction and associated theta function identities in Ramanujan's lost notebook* (to appear).
11. S.–Y. Kang, *Ramanujan's formulas for the explicit evaluation of the Rogers–Ramanujan continued fraction and theta–functions* (to appear).
12. K. Ono, S. Robins, and P. T. Wahl, *On the representation of integers as sums of triangular numbers*, Aequa. Math. **50** (1995), 73–94.
13. S. Raghavan and S. S. Rangachari, *On Ramanujan's elliptic integrals and modular identities*, Number Theory and Related Topics, Oxford University Press, Bombay, 1989, pp. 119–149.
14. S. Ramanujan, *Notebooks (2 volumes)*, Tata Institute of Fundamental Research, Bombay, 1957.
15. S. Ramanujan, *Collected Papers*, Chelsea, New York, 1962.
16. S. Ramanujan, *The Lost Notebook and Other Unpublished Papers*, Narosa, New Delhi, 1988.
17. R. A. Rankin, *George Neville Watson*, J. London Math. Soc. **41** (1966), 551–565.
18. R. A. Rankin, *Ramanujan's manuscripts and notebooks, II*, Bull. London Math. Soc. **21** (1989), 351–365.
19. S. H. Son, *Some theta function identities related to the Rogers–Ramanujan continued fraction*, Proc. Amer. Math. Soc. (to appear).
20. S. H. Son, *Cubic identities of theta functions*, The Ramanujan J. (to appear).
21. S. H. Son, *Some integrals of theta functions in Ramanujan's lost notebook*, Proceedings of the Fifth Canadian Number Theory Association Meeting (R. Gupta and K. S. Williams, eds.), American Mathematical Society, Providence, RI (to appear).
22. S. H. Son, *Septic theta function identities in Ramanujan's lost notebook* (to appear).
23. S. H. Son, *Two theta function identities in Ramanujan's lost notebook* (to appear).
24. G. N. Watson, *Theorems stated by Ramanujan (VII): Theorems on continued fractions*, J. London Math. Soc. **4** (1929), 39–48.
25. E. T. Whittaker and G. N. Watson, *A Treatise on the Theory of Bessel Functions, 2nd ed.*, Cambridge University Press, Cambridge, 1966..

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, Illinois 61801, USA

E-mail address: berndt@math.uiuc.edu

A. Schinzel

Exponential congruences.

Exactly 60 years ago Skolem made a fundamental conjecture about exponential congruences which runs as follows

Conjecture (Skolem 1937). Let K be a finite extension of $\mathbb{Q}$ and $\beta_{hi} \in K$, $\alpha_{hij} \in K^*$ $(1 \le h \le g, 1 \le i \le l, 1 \le j \le k)$. If the system of congruences

$$\sum_{h=1}^{g} \beta_{hi} \prod_{j=1}^{k} \alpha_{hij}^{x_j} \equiv 0 \pmod{m} \qquad (1 \le i \le l)$$

is solvable for all ideals m of K, then the corresponding system of equations is solvable in integers.

Skolem himself has proved the conjecture for the case $g=2$, $\alpha_{1ij}=1$, $\alpha_{2ij}=\alpha_{2j}$ for all i,j. This is a special case of the following

Theorem 1. Let $f_i(z_1,\dots,z_q)$ $(1 \le i \le l)$ be polynomials over K, $\alpha_{pj} \in K^*$ $(1 \le p \le q, 1 \le j \le k)$ and $M \in \mathbb{N} = \{1,2,\dots\}$. If the system of equations $f_i(z_1,\dots,z_q)=0$ $(1 \le i \le l)$ has only a finite number of solutions in $\mathbb{C}$ and the system of congruences

$$f_i\Big(\prod_{j=1}^{k} \alpha_{1j}^{x_j}, \dots, \prod_{j=1}^{k} \alpha_{qj}^{x_j}\Big) \equiv 0 \pmod{m}$$

is solvable for all moduli m prime to M, then the corresponding system of equations is solvable in integers.

In some special cases the moduli m can be restricted to prime ideals. Here are ~~two such theorems~~ some such results.

Theorem 2. Let $f \in K[x]$ be of degree d, $\alpha_1,\dots,\alpha_k \in K^*$. If the congruence

$$(*) \qquad f\Big(\prod_{j=1}^{k} \alpha_j^{x_j}\Big) \equiv 0 \pmod{\mathfrak{p}}$$

is solvable for almost all prime ideals $\mathfrak{p}$ of K, then the corresponding equation is solvable in rationals with the least common denominator not exceeding $\max\{1, d-1\}$.

Corollary 1 If $d \neq 2$ solvability of (*) for almost all prime ideals $\mathfrak{p}$ of K implies solvability of the corresponding equation in integers.

For $d = 3$ Corollary 1 fails, as is shown by the following

Example 1 $f(t) = (t-\beta_1)(t-\beta_2)(t-\beta_1\beta_2)$,

where $\beta_1, \beta_2 \in K$ are multiplicatively independent and $\alpha_i = \beta_i^2$ $(i=1,4$.

Corollary 2. Let $\{F_n\}$ be the Fibonacci sequence. If a congruence

$$F_n \equiv a \pmod{p}$$

is solvable for almost all primes p, then $a = F_k$ with $k \in \mathbb{Z}$.

To deduce Corollary 2 from Theorem 2 one takes $K = \mathbb{Q}(\sqrt{5})$

$$f(t) = (t^2 - a\sqrt{5}t + 1)(t^2 - a\sqrt{5}t - 1), \quad \alpha_1 = \frac{1+\sqrt{5}}{2}.$$

Problem 1. Assume that $F_{3n} \equiv a \pmod{p}$ is solvable for all primes p. Does it follow that $a = F_{3k}$, $k \in \mathbb{Z}$?

Theorem 3 Let $\alpha_{ij}, \beta_i \in K^*$ $(1 \leq i \leq l, 1 \leq j \leq k)$ and assume that for at least one i the numbers α_{ij} are multiplicatively independent. If the system of congruences

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \pmod{\mathfrak{p}} \quad (1 \leq i \leq l)$$

is solvable for almost all prime ideals $\mathfrak{p}$ of K, then the corresponding system of equations is solvable in integers.

Example 2 $K = \mathbb{Q}$, $\alpha_{11} = 2$, $\alpha_{12} = 3$, $\alpha_{13} = 1$, $\beta_1 = 1$

$$\alpha_{21} = 1, \alpha_{22} = 2, \alpha_{23} = 3, \beta_2 = 4$$

shows that the assumption about multiplicative independence in Theorem 3 is necessary even if $\mathfrak{p}$ runs through all prime ideals of K.

Theorem 3 implies the following ~~Corollary~~.

Corollary 3. Let $\alpha_{1}, \ldots, \alpha_{l}, \beta_1, \ldots, \beta_l \in K^*$. If the system of congruences

$$\alpha_i^x \equiv \beta_i \pmod{\mathfrak{p}} \quad (1 \leq i \leq l)$$

is solvable for almost all prime ideals $\mathfrak{p}$ of K, then the corresponding ~~equation~~ system of equations is solvable in integers.

In Theorems 2 and 3 and in Corollaries 1,2,3 almost all prime ideals (or primes) means all except a set of Dirichlet's density zero. Then in particular, Corollary 1 implies that if $a, b \in \mathbb{Q}^\wedge$ and $b \neq a^k$, then the lower density of primes p such that $p \mid a^n - b$ for some n, is less than 1. Very recently, two Dutch mathematicians P. Moree and P. Stevenhagen have determined exactly the density of such primes, however on the assumption of an extended Riemann hypothesis.

Corollary 3 ~~implies~~ easily implies

Corollary 4 Let $\alpha_1, \dots, \alpha_l, \beta_1, \dots, \beta_l \in K^*$, P be the set of prime ideals of K. The implication

$$\overset{\forall}{n_1,\dots,n_l \in \mathbb{N}} \quad \overset{\dot\forall}{\mathfrak{p} \in P} \quad \mathfrak{p} \mid \alpha_1^{n_1} \dots \alpha_l^{n_l} - 1 \Longrightarrow \mathfrak{p} \mid \beta_1^{n_1} \dots \beta_l^{n_l} - 1$$

holds if and only if there exists an integer e such that

$$\beta_i = \alpha_i^e \quad (1 \le i \le l).$$

($\overset{\dot\forall}{\mathfrak{p} \in P}$ means "for almost all $\mathfrak{p} \in P$").

A proof appeared recently in volume 2 of Matematicheskiye zapiski dedicated to the memory of N.I. Feldman. The special case $l = 1$ was proved earlier, although published later by C. Corrales-Rodrigáñez and R. Schoof. Now I shall present still unpublished results in the same direction obtained jointly with two French mathematicians, D. Barsky and J.-P. Bézivin. To state these results I need some ~~notation~~

Notation. Γ_n is the multiplicative group of nth roots of unity.

$$\Gamma = \bigcup_{n=1}^{\infty} \Gamma_n, \quad \Gamma_w = \Gamma \cap K.$$

For a polynomial $F \in K[x_1, \dots, x_n]$

$$\Omega(F) = \{ \langle \gamma_1, \dots, \gamma_n \rangle \in \Gamma^n : F(\gamma_1, \dots, \gamma_n) = 0 \}.$$

Theorem 4 Assume that $R \in K[x_1,\dots,x_r]$, $S \in K[x_1,\dots,x_s]$, $\Omega(R) \neq \emptyset$ and $\Omega(S)$ is finite. Let $\alpha_1,\dots,\alpha_r,\beta_1,\dots,\beta_s \in K^\times$ and $\alpha_1,\dots,\alpha_r$ be multiplicatively independent. If

$$\bigvee_{n\in\mathbb{N}} \overset{\infty}{\bigvee_{\mathfrak{p}\in P}} \mathfrak{p} \mid R(\alpha_1^n,\dots,\alpha_r^n) \Longrightarrow \mathfrak{p} \mid S(\beta_1^n,\dots,\beta_s^n),$$

then there exist integers $e>0$ and d_{ij} such that

$$\beta_i^e = \prod_{j=1}^{r} \alpha_j^{d_{ij}} \qquad (1 \le i \le s).$$

Corollary 5 Let $w=2$ and $\alpha_1,\alpha_2,\beta_1,\beta_2$ be integers of K. Assume that neither $\pm\alpha_i$, nor $\pm\beta_i$ $(i=1,2)$ is a unit or a perfect power in K and that $(\alpha_1,\alpha_2) = (\beta_1,\beta_2) = 1$. The implication

$$\mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Longrightarrow \mathfrak{p} \mid \beta_1^n + \beta_2^n + 1$$

holds if and only if $\{\beta_1,\beta_2\} = \{\alpha_1,\alpha_2\}$.

The difficult "only if" part of Cor. 5 can be deduced from Theorem 4 as follows. Take $R = S = x_1 + x_2 + 1$. We have $\Omega(R) = \Omega(S) = \{\langle \xi_3, \xi_3^2\rangle, \langle \xi_3^2, \xi_3\rangle\}$, so that the assumption concerning Ω's in Theorem 4 is satisfied. Since α_1, α_2 are integers, different from units and relatively prime, they are multiplicatively independent. Thus Theorem 4 applies and gives

$$\beta_i^e = \alpha_1^{d_{i1}} \alpha_2^{d_{i2}} \qquad (i=1,2)$$

Since also β_i are integers and relatively prime we have either $d_{12} = d_{21} = 0$ or $d_{11} = d_{22} = 0$. Permuting α_1, α_2, if necessary, we may assume that

$$\beta_i^e = \alpha_i^{d_{ii}} \qquad (i=1,2).$$

Since $w=2$ this equality implies that either one of the numbers $\pm\alpha_i, \pm\beta_i$ is a perfect power in K, or

$$\beta_i = \varepsilon_i \alpha_i \ , \ \varepsilon_i \in \{1,-1\} \ (i=1,2).$$

Now, we take n odd and remember that

$$\mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Rightarrow \mathfrak{p} \mid \beta_1^n + \beta_2^n + 1.$$

We get

$$\mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Rightarrow \mathfrak{p} \mid \varepsilon_1 \alpha_1^n + \varepsilon_2 \alpha_1^n + 1.$$

If $(\varepsilon_1, \varepsilon_2) \neq (1,1)$, adding, or subtracting we get $\mathfrak{p} \mid 2\alpha_1^n$, or $\mathfrak{p} \mid 2\alpha_2^n$, or $\mathfrak{p} \mid 2$, which is possible only for finitely many prime ideals $\mathfrak{p}$. Since, by an old theorem of Pólya, there are infinitely many prime ideals $\mathfrak{p}$ dividing $\alpha_1^n + \alpha_2^n + 1$ for some odd n, we infer that $\varepsilon_i = 1$, i.e. $\beta_i = \alpha_i$ $(i=1,2)$.

Corollary 5 suggests the following problems.

Problem 2 Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K^*$ and assume that

$$\forall_{n \in \mathbb{N}} \ \forall_{\mathfrak{p} \in P} \ \mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Leftrightarrow \mathfrak{p} \mid \beta_1^n + \beta_2^n + 1.$$

Is it true that $\{\beta_1, \beta_2\} = \{\alpha_1, \alpha_2\}$ or $\{\alpha_1^{-1}, \alpha_2^{-1}\}$?

The example $\alpha_2 = \alpha_1^2$, $\beta_i = \alpha_i^{-1}$ $(i=1,2)$ shows that the second term of the alternative is really needed.

Problem 3. Disprove the statement

$$\exists_{p_0} \ \forall_{p > p_0, \ p \text{ prime}} \ \forall_{n \in \mathbb{N}} \ p \mid 2^n - 3 \Leftrightarrow p \mid 3^n - 2.$$

P. Stevenhagen solved Problem 3 assuming an extended Riemann hypothesis.